

米国におけるデータの保護および国際間移転

小田哲明 (立命館大学大学院 テクノロジー・マネジメント研究科 教授)

クリス ミズモト (ミズモト外国法事務弁護士事務所 米国弁護士 (ニューヨーク州, カリフォルニア州, 米国特許商標庁)/ 外国法事務弁護士 (日本))

Data Protection in the US and International Transfer of Data

Tetsuaki Oda

Professor, Graduate School of Technology Management, Ritsumeikan University

Chris Mizumoto

Foreign Law Office of Chris Mizumoto, Attorney at law in NY, CA, Japan, and USPTO

【要旨】 米国において、非パーソナルデータについては、営業秘密、コンピュータ不正アクセスに関する刑法、特許権、著作権、契約により主に保護される。パーソナルデータの保護については、金融サービス、医療保険、児童保護等の分野ごとに連邦法が定められており、個人情報の保護について州法を成立させた州もある。米国と他国のパーソナルデータの国際間移転については、米国はEU-US プライバシーシールドやAPEC 越境プライバシールールに合意し、プライバシーデータの国際間移転を促す国際的枠組の構築を図っている。重要技術等の重要データについては、2019 年度の国防権限法を成立させ、外国企業の投資による米国企業の支配の制限を強化し、輸出・再輸出の制限対象を重要技術に拡大している。

【キーワード】 データ保護 パーソナルデータ / 非パーソナルデータ 産業データ データ国際間移転

【Abstract】 In the US, non-personal data are mainly protected by trade secret, criminal law on inequitable access to computer, patent rights, copyrights, and contracts. On the other hand, personal data are protected by federal laws in categories such as financial service, health insurance, children protection, and so forth, while some states have enacted personal information protection acts. With regard to the international transfer of data between the US and another country, the US has agreed to an EU-US privacy shield and APEC cross-border privacy rules to establish a framework for advancing international transference. The US enacted the National Defense Authorization Act for fiscal year 2019 for important data of critical technologies to strengthen the oversight of businesses in the US by foreign businesses and enlarge the subject of restriction on export and reexport to include those data of the critical technologies.

【Keywords】 Data Protection Personal Data / Non-personal Data Industry Data International Transfer of Data

1. はじめに

通信技術の発達やデータビジネスの拡大により、データが持つ価値は年々増大している。また、ビッグデータを処理する人工知能の発達により、マーケ

ティング・製造・医療・金融などの様々な分野でデータの有益な活用が望まれている。一方、GAFA¹等のデータプラットフォーマー（または、デジタルプラットフォーマー）が現れ、ネットワーク外部性²により、パーソナルデータが特定の企業に集中している。このように、デジタル革命を背景に第4次産

業革命と呼ばれる新しい産業が生まれ、国際的にもデジタル貿易が拡大する中、プライバシーや安全保障の観点からパーソナルデータや重要データの流通を制限するとともに、データを有効に活用するためにデータの国際間移転を促す国際的枠組の構築を図っている。

米国は、GAFA等の巨大データプラットフォームを擁するため、パーソナルデータに関してはある程度のプライバシーを確保したうえで各社による自主規制に任せ、データをできるだけ自由に活用させようとするスタンスが強く、重要技術等の重要データに関しては安全保障や自国産業保護の観点から国外流出を厳しく制限するスタンスが強い。

2. データの分類

データの分類には様々な類型があり、例えば、総務省平成29年度版情報通信白書では、①国や地方公共団体が提供するオープンデータ、②企業の暗黙知（ノウハウ）をデジタル化・構造化したデータ（知のデジタル化データ）、③企業活動によってM2M（Machine to Machine）から吐き出されるストリーミングデータ（M2Mデータ）、および④個人の属性に係るパーソナルデータに分類し、②知のデジタル化データおよび③M2Mデータを「産業データ」として位置付けている。

「産業データ」には、農業やインフラ管理からビジネス等に至る産業や企業が持ちうるパーソナルデータ以外のデータ、工場等の生産現場におけるIoT機器から収集されるデータ、橋梁に設置されたIoT機器からのセンシングデータ（歪み、振動、通行車両の形式・重量など）等が含まれる（「総務省平成29年度版情報通信白書」参照）。

「パーソナルデータ」には、個人の属性情報、移動・行動・購買履歴、ウェアラブル機器から収集された個人情報その他、特定の個人を識別できないように加工された人流情報、商品情報等も含まれる（「総務省平成29年度版情報通信白書」参照）。

本稿では、パーソナルデータとそれ以外の非パーソナルデータ（国や地方自治体の機密データ、産業データ、技術情報を含む）について説明する。表1

には米国におけるデータの保護制度についてまとめている。表2には米国と他国におけるデータの国際間移転についてまとめている。

3. 米国の法制度

米国は第一次的法源として判例法主義を採用しており、同一管轄の上級裁判所に同様の先例がある場合は、その先例に従って裁判を行わなければならないという先例拘束の原則がある。

また、米国では、法的救済について、コモンローに基づく救済とエクイティに基づく救済に区別される。コモンローに基づく救済は金銭による損害賠償であり、エクイティに基づく救済は差止命令や特定履行（契約上の義務を履行させること）による救済等である。例えば、コモンローに基づく金銭的損害賠償では損害の回復が不十分である場合、衡平の観点から、エクイティに基づく差止命令や特定履行による救済が図られ、より柔軟で裁判官の裁量が広い運用がなされている。ここで注意しておきたいのが、米国における民事的救済は、一般的に、コモンローに基づく金銭的損害賠償を原則としており、エクイティに基づく差止命令や特定履行による救済は、金銭的損害賠償では損害の回復が不十分である場合に限られる点である。例えば、実務的に契約上エクイティに基づく救済の義務を課したとしても、必ずしも裁判所で認められるとは限らない。

また、米国では連邦制が採用されており、連邦法と州法が区別され、連邦裁判所と州裁判所がそれぞれ設置されている。連邦裁判所を専属管轄として規定されている事件（特許権、商標権、著作権等に関する事件）は連邦裁判所の管轄となり、それ以外の連邦法や条約に基づく事件、および異なる州の市民間（州民と外国人を含む）の訴訟で訴額が一定以上の事件は、連邦裁判所を管轄とすることができる。

4. 米国における非パーソナルデータの保護

4.1. 営業秘密としての保護

4.1.1. 州法

営業秘密は、先例拘束の原則の下コモンローに基づいて、不法行為に対する民事的救済により保護されてきた。また、営業秘密保護の統一的な見解を示すモデル法として、不法行為法リステイトメント（1939年制定）および統一営業秘密法：UTSA（Uniform Trade Secret Act）（1979年制定）があり、各州が採択することで州法として制定されている。

UTSAは、州間における営業秘密の保護要件や救済の差異を是正するものであり、営業秘密や営業秘密の不正取得の定義、差止請求、損害賠償請求、および懲罰的損害賠償等を規定しているが、各州の採択において内容が変更されたり、解釈が異なったりする場合があるため、注意を要する。

UTSAを要約すれば、営業秘密は、非公知性、秘密保持のための合理的措置、および独立した経済的価値を備える情報（製法、パターン、編集物、装置、方法、技術、またはプロセスを含む）であって、営業秘密の不正取得は、不当な手段（窃盗、贈収賄、スパイ行為など）で取得された営業秘密であることを知ってまたは知り得べき理由があるにもかかわらず取得すること、不適切な手段を用いて取得した営業秘密を同意なしに開示または使用すること等であると規定されている。UTSAに示される救済手段として、差止請求、損害賠償請求（故意および悪意の場合は2倍までの懲罰的損害賠償を含む）、および故意および悪意の場合は弁護士費用請求が認められる。なお、秘密保持のための合理的措置としては、アクセス制限のみでは足りず、営業秘密であることの明記（例えば、confidentialの明記）やアクセスした営業秘密の処理（例えば、閲覧後速やかに破棄する）が必要となる。

4.1.2. 連邦法

国際的な軍事技術情報のスパイ事件や営業秘密のデジタル化等を背景に、統一的に営業秘密の保護強化を図るため、刑事的制裁を課す連邦経済スパイ

法：EEA（Economic Espionage Act of 1996）（1996年制定）および民事的救済を図る連邦営業秘密保護法：DTSA（Defend Trade Secret Act）（2016年制定）が制定された。

EEAにおいて、営業秘密は、UTSAとほぼ同様であるが、金融・ビジネス・科学・技術・経済・工学における情報（パターン、計画、編集物、プログラム機器、製法、設計、試作品、方法、技術、プロセス、手続、プログラム、またはコードを含む）であり、有形無形を問わず、物理的または電子的等の情報の固定手段を問わない。

刑事的制裁を課すEEAにより、外国政府に利益を与える営業秘密を認識または意図して不正取得（未遂や共謀を含む）した場合、個人に対しては50万ドル以下の罰金または／および15年以下の懲役が科され、企業に対しては1000万ドル以下の罰金が科される。また、営業秘密の所有者（正当なライセンシーを含む）に損害を与えることを認識または意図して製品に係る営業秘密を不正取得（未遂や共謀を含む）した場合、個人に対しては罰金または／および10年以下の懲役が科され、企業に対しては500万ドル以下の罰金が科される。また、営業秘密の不正取得の結果により得た財産や営業秘密の不正取得のために用いられる財産を没収する規定が定められている。

DTSAにおいて、営業秘密は、UTSAとほぼ同様である。営業秘密の所有者（正当なライセンシーを含む）は営業秘密の不正取得について連邦裁判所に民事上の救済を求めることができる。

DTSAに示される救済手段として、不正取得された営業秘密の拡散を防止するために、当事者の申し立てにより、一定の条件の下、裁判所は事前通告なしの財産の差押命令（ex-parte seizure）を発することができる。また、差止請求、損害賠償請求（故意および悪意の場合は2倍までの懲罰的損害賠償を含む）、および故意および悪意の場合は弁護士費用請求が認められる。

DTSAでは、政府機関や裁判所に法令違反を通告（公益通報）する際に営業秘密を開示する場合、営業秘密の開示について民事的責任および刑事的責任を免れる旨が規定されている。また、使用者は、営

業秘密や秘匿情報を管理する従業者（契約者やコンサルタントを含む）に対してすべての契約書や合意書において、この免責を通知しなければならない、これに反する場合、当該従業者に対する損害賠償請求や弁護士費用請求を行なうことができない可能性がある。

また、DTSA では、州法と抵触しない限り、使用者は従業者の転職を妨げることができない。ただし、営業秘密の不正取得のおそれがあることを証明できる（単に営業秘密を知っているという情報だけでは足りない）場合には、使用者は従業者の転職を妨げることができる可能性がある。なお、営業秘密の不正取得の証明に関し、不正取得後に使用者が従業者の Facebook を無断で閲覧したことがクリーンハンズの法理やプライバシーに反しないとして許容された米国控訴裁判所の判例がある。

4.2. コンピュータ（記憶媒体や通信機器を含む）への不正アクセスからの保護

権限なくまたは権限を越えてコンピュータに不正にアクセスした場合、連邦法の刑法 1030 条に違反することになり、罰金や懲役が科される。刑法 1030 条は、総合犯罪規制法：CCCA（Comprehensive Crime Control Act）（1984 年制定）およびコンピュータ犯罪取締法 CFAA（Computer Fraud and Abuse Act）（1986 年制定）により修正され、現在の規定になっている。これにより厳罰が科されることとなったため、データを取り扱う際に、契約においてアクセス権限の範囲等について注意する必要がある。

4.3. 特許権による保護

米国特許審査マニュアルである MPEP（Manual for Patent Examination Procedure）によれば、物理的有形的要素を伴わないデータ自体やコンピュータプログラム自体は、特許法 101 条に規定されている法定主題（Statutory Subject Matter）の製品（Product）とはならない。また、物理的有形的要素を伴うデータであっても、判例上の例外（抽象的アイデア、自然現象、または自然法則）であり、且つ他の要素が判例上の例外を著しく超えるものでなければ、特許適格性（Patent Eligibility）を有さない（Alice/Mayo

test）。さらに、特許として保護されるためには、新規性や非自明性等の特許要件を満たす必要があり、データ自体に価値がある場合、特許権による保護は限定的になる可能性がある。なお、データの処理方法は、特許法 101 条に規定されている法定主題であり、Alice/Mayo test を満たせば特許適格性を有する。

4.4. 著作権による保護

全体として創作的な著作物を構成する方法で、既存のデータを選択し、整理しまたは配列し、これらを収集し編成して作られた編集著作物（集合著作物を含む）は、著作物として著作権により保護される。また、Feist 連邦最高裁判決以降、著作物の創作性の要件として、編集者の労力に報いる「額に汗（sweat of the brow）」の理論ではなく、最低限度の創造性（minimal degree of creativity）が要求されることとなった。したがって、編集著作物としてではなくデータ自体に価値がある場合、著作権による保護は限定的になる可能性がある。なお、データがコンピュータプログラムである場合は、コンピュータプログラムの著作物として著作権による保護を受けることができる。

また、デジタルミレニアム著作権法：DMCA（Digital Millennium Copyright Act）（1998 年制定）により、著作権法の一部が改正され、著作物のコピーコントロールの回避を規制するとともに、著作物へのアクセスコントロールを回避する（スクランブルや暗号化を解除等する）技術、装置、サービスを禁止し、著作権を侵害するか否かを問わず、アクセスコントロールの回避行為を禁止している。また、DMCA では、インターネットサービスプロバイダー（ISP）が著作権侵害に対してコンテンツの削除等の一定の対処を行なうことで責任を免れるセーフハーバーが規定されている。

4.5. 契約による保護

データを保護するために、データの所有権、データの利活用、営業秘密の取り扱い、秘密保持、およびアクセス権限等について契約を締結し、契約違反に該当する場合の損害賠償請求や差止請求について

規定することが一般的である。契約違反に該当する場合、コモンローに基づく金銭的損害賠償が原則であり、エクイティに基づく差止命令や特定履行は、金銭的損害賠償では損害の回復が不十分である場合に限られ、必ずしも裁判所で認められない点に注意する。

5. 米国におけるパーソナルデータの保護

5.1. 連邦法

米国には、我が国の個人情報の保護に関する法律（個人情報保護法）のような包括的な連邦法は存在せず、特定の分野ごとにパーソナルデータを保護する連邦法が制定されている。例えば、プライバシー法（Privacy Act of 1974）、公正信用報告法：FCRA（Fair Credit Reporting Act）、金融サービス近代化法：GLBA（Gramm-Leach-Bliley Act）、医療保険の相互運用性と説明責任に関する法律：HIPAA（Health Insurance Portability and Accountability Act）、児童オンラインプライバシー保護法：COPPA（Children's Online Privacy Protection Act）がある。

2019年2月、中国発のリップシンク動画アプリであるTikTokが、児童の個人情報を保護者の同意なしに収集していたとして、COPPA違反による過去最高額の制裁金570万ドルで連邦取引委員会：FTC（Federal Trade Commission）と和解したと発表された。

パーソナルデータに関して上記のような連邦法が及ばない範囲についても、各企業が自ら公表したプライバシーポリシーを遵守する等、自主規制による

保護を基本とし、連邦取引委員会法5条「不公正又は欺瞞的な行為又は慣行」に該当する場合に、FTCが制裁金を課したり差止命令を発したりすることができる。

また、パーソナルデータの包括的な保護を目指して、消費者プライバシー権利章典：CPBR（Consumer Privacy Bill of Rights）の法案が2015年2月に公表され（2012年2月草案公表）、消費者によるパーソナルデータのコントロール権等が謳われているが、2019年4月現在、法制化されていない。また、消費者プライバシーやパーソナルデータの保護に関する様々な法案が上院および下院に提出されている。

5.2. 州法

パーソナルデータ保護の流れの中、カリフォルニア州議会がカリフォルニア州消費者プライバシー法：CCPA（California Consumer Privacy Act of 2018）を2018年6月に可決した（2020年1月1日施行予定）。CCPAでは、消費者はカリフォルニア州で事業を行なう事業者に対し、事業者が収集した個人情報（パーソナルインフォメーション）のカテゴリ、具体的な個人情報、個人情報収集・販売の目的、個人情報を共有する第三者の開示を要求でき、個人情報の削除を要求することができる。また、個人情報の収集に際し、事業者は消費者に対し、収集する個人情報のカテゴリーや収集の目的を知らせなければならない。ここで言う事業者は、以下の①～③のうち少なくとも1つを満たす事業体である。①年間総収益が2500万ドルを超える。②商目的で年間5万件以上の個人情報を取引する。③個人情報の

表1 米国におけるデータの保護制度

非パーソナルデータの保護					パーソナルデータの保護	
営業秘密		コンピュータ不正アクセス	特許権・著作権	契約	自主規制を基本とした保護	
連邦法	州法	連邦法	連邦法	州法	連邦法（分野ごと）	州法
■ EEA ■ DTSA	■ モデル法（不法行為法リステイメントおよびUTSA）	■ 刑法1030条（CFAAおよびCFAAにより修正）	■ 特許法 ■ 著作権法（DMCA）	■ 損害賠償請求 ■ 差止請求	■ Privacy Act of 1974 ■ FCRA ■ GLBA ■ HIPAA ■ COPPA ■ CPBR	■ カリフォルニア州 ■ ネバダ州 ■ ミネソタ州

売却益が年間総収入の 50% 以上を占める。さらに、消費者は、事業者が個人情報を販売することからオプトアウトできる権利を有し、オプトアウトした消費者は事業者による差別的な扱いを受けない。なお、CCPA の運用規則は、パブリックコメントや複数のパブリックフォーラムを経て公表される。

その他、ネバダ州とミネソタ州では、消費者が開示に同意した場合を除き、インターネットサービスプロバイダー（ISP）が消費者に関する情報を秘匿しなければならない。両州ともに、個人特定情報の開示を禁止しているが、ミネソタ州ではさらに、ネット閲覧行動やネット閲覧サイトについて、ISP は開示前に消費者の同意を得なければならない。他の州においても ISP に関するプライバシー法が提案されていたが、ISP の反対により否決され成立には至っていないケースが多々見受けられる。

6. 米国と他国におけるデータの国際間移転

6.1. 非パーソナルデータの国際間移転

2017 年 6 月に中国で施行されたサイバーセキュリティ法 37 条に見られるように、データの海外流出を制限し、国内に留めようとする「データローカライゼーション」の動きが進んでいる。データローカライゼーションが進展しているが、データを有効に活用するため、国際間移転（越境）の枠組も話し合われている。米国離脱後、2018 年に署名された環太平洋パートナーシップに関する包括的及び先進的な協定：CPTPP（Comprehensive and Progressive Agreement for Trans-Pacific Partnership、通称 TPP11）では、個人情報を保護しつつ、サーバーおよびストレージを自国内に設置することを要求したり、ソフトウェアのソースコード開示を要求したりすることを、原則禁止している。

一方、米国連邦政府機関のデータについて、米国の国税庁発行のガイドラインによれば、米国連邦政府機関は税務情報の処理システムを米国領域内に設置するように規定している。また、米国防省の規則では、米国防省のデータを扱うクラウドサービスプロバイダーは当該データを国内に留めておくように

規定している。

また、米国では、2019 年度の国防権限法：NDAA（National Defense Authorization Act）が成立し、これに含まれる外国投資リスク審査現代化法：FIR-RMA（Foreign Investment Risk Review Modernization Act of 2018）および輸出管理改革法：ECRA（Export Control Reform Act of 2018）も成立した。特に、中国によるインフラ支配や技術流出に対する懸念を視野に入れた法律となっている。

FIR-RMA では、外国企業の投資による米国企業の支配等について安全保障上問題がないかを審査する外国投資委員会：CFIUS（Committee on Foreign Investment in the United States）の審査対象や権限を強化することで、外国企業の投資により米国企業が保有する重要インフラや重要技術や機密性の高いパーソナルデータが海外に流出するリスクを低減することができるようになった。未施行である FIR-RMA の一部規定については、パイロットプログラムが 2018 年 11 月 10 日から開始されている。

ECRA では、輸出・再輸出の制限対象となる重要技術に新興・基盤的技術（emerging and foundational technologies）が含まれるようになり、以下の技術についてパブリックコメントを求めている。①バイオテクノロジー②人工知能および機械学習③測位技術④マイクロプロセッサ⑤先進的コンピューティング⑥データ分析⑦量子情報および量子センシング技術⑧ロジスティクス⑨ 3D プリンティング⑩ロボティクス⑪ブレインコンピューターインターフェース⑫超音速⑬先進的材料⑭先進的監視技術

6.2. パーソナルデータの国際間移転

2018 年 5 月に欧州で施行された一般データ保護規則：GDPR（General Data Protection Regulation）に見られるように、パーソナルデータの保護強化やパーソナルデータのデータローカライゼーションの動きが進んでいる。GDPR は欧州経済領域：EEA（European Economic Area）居住者のパーソナルデータを取得したり処理したりする場合に適用されるため、EU 域外の企業に対しても、2000 万ユーロまたは全世界売上高 4% の何れか高い方を上限とする制裁金が科されるおそれがある。2019 年 1 月、パー

ソナルデータの透明性および情報提供義務に違反し、ユーザーの同意なしに広告パーソナライゼーションを行なったとして、グーグルがGDPRに基づき5000万ユーロの罰金支払いを命じられたと発表された。

パーソナルデータの保護が十分であると欧州委員会が認定した国や地域においては、EU居住者のパーソナルデータの国際間移転を認めており、日本は2019年1月に十分性の認定を受けた。

米国は、欧州委員会の十分性の認定を受ける代わりに、EU-US プライバシーシールド（欧州司法裁判所により無効とされたセーフハーバー協定を見直したもの）により、欧州委員会とパーソナルデータの国際間移転に合意している。EU-US プライバシーシールドでは、EU居住者のパーソナルデータを米国に移転する際の政府および企業の義務を強化し、米国企業は、米商務省に認定されてリストに登録されれば、EU居住者のパーソナルデータを米国に移転することができる。なお、EUに加盟していないスイスと米国の間では、Swiss-US プライバシーシールドによりパーソナルデータの国際間移転が合意されている。

日本および米国が参加しているアジア太平洋経済協力会議：APEC は、越境したパーソナルデータの漏洩等について自国の法令を円滑に執行できるよう、情報提供や調査協力を他国に依頼できる越境プライバシー執行協力協定：CPEA（Cross-Border Privacy Enforcement Agreement）を2009年に成立させている。2019年4月現在、オーストラリア、ニュージーランド、米国、香港、カナダ、韓国、メキシコ、シンガポール、日本、フィリピン、台湾がCPEAに参加している。また、APEC は、パーソナルデータの国際間移転について、2011年に越境プ

ライバシールール：CBPR（Cross-Border Privacy Rules）を成立させ、2019年4月現在、米国、メキシコ、日本、カナダ、韓国、シンガポール、台湾がCBPRに参加している。CBPRでは、所定の認証機関の審査により認証されれば、企業はパーソナルデータをAPEC参加国に円滑に移転することができる。

7. 課題

欧州議会は、拘束力はないが、EU-US プライバシーシールドの停止を求める決議を2018年7月に行なった。EU-US プライバシーシールドの登録企業であるFacebookの数千万人のユーザーデータがケンブリッジアナリティカに流出し、2016年米国大統領選挙やブレグジットに影響を与えた疑惑があることが2018年3月に発覚した事件が、この議論に拍車をかけた。このように、データ保護の実効性に関しては未だ国際間の隔たりがあるが、国際的な枠組によりデータ保護のハーモナイゼーションが進むとともに、データ保護の実効性も図られていくであろう。また、データの保護・流通が貿易交渉において語られるようになり、データの保護・流通が今後さらに重要な交渉マターとなるであろう。

ハーバード大学のマイケル・ポーター教授は、データの流通により既存のバリューチェーンが大きく変化すると唱えている。変化するバリューチェーンの中で我が国の産業がどの部分に付加価値を創出できるのかを考え、国際的な立ち位置を見極める必要がある。巨大プラットフォームによるデータの収集・活用に強みを持つ米国、通信インフラに強みを持ち且つ巨大データプラットフォームが出現してきた中国、および我が国が製品やサービスを展開している（または、展開を予定している）その他の国とどのように関係を構築していくかが課題である。

表2 米国と他国におけるデータの国際間移転

データ ローカライゼーション	パーソナルデータの国際間移転	
	欧州	APEC
■税務情報 ■国防省データ ■FIRIMA ■ECRA	■EU-US プライバシーシールド ■Swiss-US プライバシーシールド	■CPEA ■CBPR

注

- 1 Google, Apple, Facebook, Amazonの頭文字を取った主要IT企業の総称。なお、中国のデータプラットフォームをBAT（Baidu, Alibaba, Tencentの頭文字。これにHuawei, JD.comを加えることもある。）と呼ぶ。
- 2 製品やサービスの価値がその製品やサービスを利用するユーザー数に依存すること。ユーザー数が閾値を超えると急激にその製品やサービスが普及し、スイッチングコストによるロックイン効果

が生じる。

参考文献

APEC “Cross-Border Privacy Enforcement Arrangement (CPEA)” (<https://cbprs.blob.core.windows.net/files/Cross%20Border%20Privacy%20Enforcement%20Arrangement.pdf>) 2019年4月18日閲覧。

APEC “Cross-Border Privacy Rules (CBPR) System” (<http://cbprs.org/>) 2019年4月18日閲覧。

California Consumer Privacy Act of 2018, California Civil Code § 1798.100.

Children’s Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501–6506 (Pub.L. 105–277, 112 Stat. 2681–728, enacted October 21, 1998).

Comprehensive Crime Control Act of 1984, Pub.L. 98–473, S. 1762, 98 Stat. 1976, enacted October 12, 1984.

Computer Fraud and Abuse Act (CFAA), enacted by Congress in 1986, which amended, 18 U.S.C. § 1030.

Defend Trade Secrets Act of 2016, Pub.L. 114–153, 130 Stat. 376, enacted May 11, 2016, codified at 18 U.S.C. § 1836, et seq.

Digital Millennium Copyright Act (DMCA), Pub. L. 105–304, 112 Stat. 2860 (1998).

Economic Espionage Act of 1996, Pub.L. 104–294, 110 Stat. 3488, enacted October 11, 1996.

Gramm-Leach-Bliley Act (GLBA), Financial Services Modernization Act of 1999, (Pub.L. 106–102, 113 Stat. 1338, enacted November 12, 1999).

Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996).

NATIONAL CONFERENCE OF STATE LEGISLATURES “Privacy

Legislation Related to Internet Service Providers-2018” Jan 16th, 2019 (<http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internet-service-providers-2018.aspx>) 2019年4月18日閲覧。

JOHN S. McCAIN “National Defense Authorization Act for Fiscal Year 2019” Aug. 2018 (<https://www.congress.gov/bill/115th-congress/house-bill/5515/text>) 2019年4月18日閲覧。

Scherer Design Group, LLC v. Ahead Engineering LLC, 18–2835 (3rd Cir. 2019).

Privacy Act of 1974 (Pub.L. 93–579, 88 Stat. 1896, enacted December 31, 1974, 5 U.S.C. § 552a).

Restatement (First) of Torts § 757, Liability for Disclosure or Use of Another’s Trade Secret—General Principle (1939) American Law Institute.

The 2019 Revised Patent Subject Matter Eligibility Guidance (issued January 7, 2019), USPTO.

THE WHITE HOUSE “CONSUMER DATA PRIVACY IN A NEW WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY” Feb. 2012 (<https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf>) 2019年4月18日閲覧。

Uniform Trade Secrets Act (Drafted by the National Conference of Commissioners on Uniform State Laws, as amended 1985), 1979.

18 USC 1030: Fraud and related activity in connection with computers, U.S. Code Title 18, CRIMES AND CRIMINAL PROCEDURE.

総務省 (2017) 『平成 29 年度版情報通信白書』。

ハーバード・ビジネス・レビュー (2016) 『IoT の衝撃』ダイヤモンド社。